EXTRAHOP®

CUSTOMER STORY

Asset Management Leader Secures Global Financial Assets and Regains Operational Control by Displacing Legacy NDR

A leading global asset manager deployed ExtraHop to close visibility gaps and regain control over its security environment. By outperforming the incumbent NDR in a Red Team exercise and identifying critical hardening issues, the firm established a unified source of truth across its global banking infrastructure.

The organization selected the ExtraHop RevealX™ platform to serve as the unified source of network truth, delivering:

- **Proven Detection Superiority:** In a head-to-head Red Team exercise, ExtraHop demonstrated clear superiority in threat detection and response over the incumbent NDR vendor.
- **Immediate Infrastructure Hardening:** The platform identified a significant number of network hardening issues and protocol vulnerabilities during the proof of concept (POC), allowing for proactive risk reduction.
- **Ecosystem Synergy:** ExtraHop provided deep integration with the firm's existing security stack, including Microsoft Sentinel EDR, Palo Alto Networks SOAR, and BlueCoat decryption.
- **Operational Independence:** By establishing an internal source of network truth, the firm gained the visibility and control necessary to oversee the security services provided by their parent group's SOC.

The Challenge: Visibility Gaps and Outsourced SOC Control

For a global leader in asset management, the complexity of a hybrid environment is compounded by the need for extreme security vigilance. The firm's existing technical landscape presented several core challenges:

Lack of Control Over Outsourced Security	With the SOC provided by the parent corporation, the local security team struggled with a lack of direct control and visibility into their own network. This created a reliance on external reporting that lacked the granular detail required for rapid internal response.
Fragmented Visibility and Extreme Concerns About Lateral Movement	The business operates with a high degree of sensitivity toward cyber threats, yet it lacked a centralized system for real-time network monitoring. This "blindness" exacerbated significant concerns about undetected lateral movement and data exfiltration within the banking subsidiary.
Failed Detection Expectations	Previous experiences with incumbent NDR tools led to skepticism regarding detection accuracy. The team required a solution that could survive a rigorous Red Team simulation to prove it could identify sophisticated post-compromise behaviors.

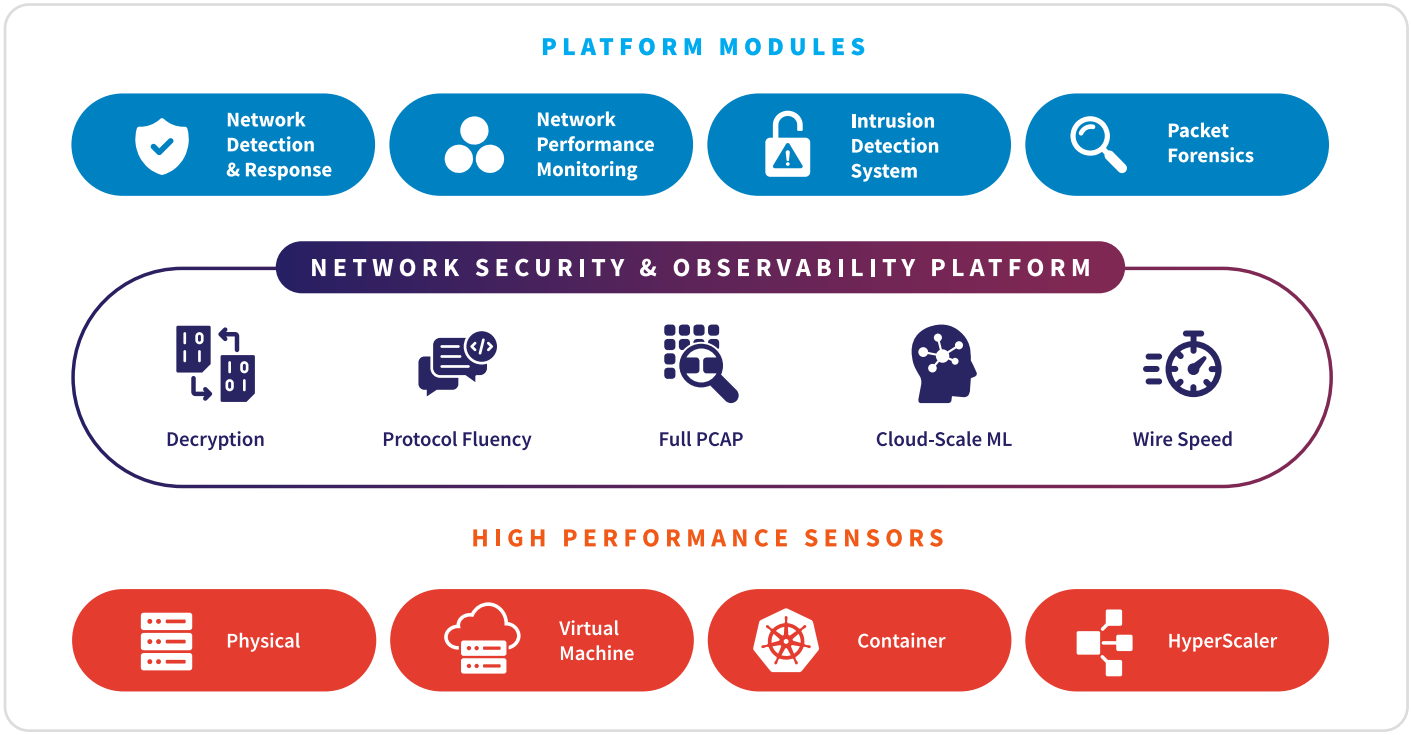
The Solution: Unified Detection with ExtraHop NDR

ExtraHop successfully provided the agentless network security solution required for a global financial environment, proving its ability to provide unified security coverage that met the firm's high-stakes requirements.

The key outcomes and advantages delivered to the exchange include:

- **Unrestricted visibility and decryption:** The global asset manager secured the required forensic depth and network control when it deployed ExtraHop, which analyzes 100 Gbps of east-west traffic and uses **high-speed decryption** to immediately find threats previously hidden within encrypted flows.
- **Reduced alert fatigue via high-fidelity detection:** The **cloud-scale machine learning** built into the ExtraHop platform lifted the SOC's operational burden because it provided high-fidelity, low-noise detections. This shift allowed analysts to move focus from low-value false positives to highly reliable network activity, signaling true post-compromise threats and **endpoint detection and response (EDR) evasion tactics**.
- **Actionable context and identity:** The security team achieved comprehensive insight by using **identity-based investigation**, which links malicious network activity directly to user and service accounts, finally enabling the detection of all missed AD and lateral movement attacks.
- **Streamlined incident response via ecosystem integration:** ExtraHop fundamentally simplified incident response workflows because it established itself as the definitive source of network truth, automatically feeding high-value contextual data to the customer's existing SIEM and EDR platforms.
- **Unified security platform:** The firm gained efficiency and reduced complexity by consolidating NDR, NPM, and IDS capabilities into **one unified, integrated solution** for comprehensive network security and observability.
- **Deep protocol coverage for core assets:** The firm mitigated major risk by gaining deep fluency (parsing over **90 protocols**) that allowed for accurate decoding of all traffic, including sensitive database communications, without introducing performance risk. This was critical for detecting hidden AD attacks and lateral movement.

ExtraHop NDR Platform



The Results: Validated Defense and Global Visibility

By deploying ExtraHop RevealX, the asset management firm transformed its defensive posture and validated its investment through real-world performance.

Decisive Red Team Victory

The platform's machine learning capabilities successfully passed a rigorous Red Team demonstration, outperforming the incumbent NDR vendor. This validation gave the firm confidence in its ability to detect sophisticated threats that previous solutions had missed.

Proactive Network Hardening

During the POC, ExtraHop identified numerous security misconfigurations and hardening issues that were previously invisible. By addressing these weak points, the team significantly reduced the internal attack surface before a full production rollout.

Integrated Security Ecosystem

The implementation successfully bridged technical gaps by integrating with F5 load balancers, BlueCoat decryption, and Microsoft Sentinel. This created a coordinated defensive posture where network truth informs every aspect of the firm's security stack.

Regained Control Over SOC Operations

With ExtraHop established as the definitive source of network truth, the firm now has the independent visibility required to manage its relationship with the parent group's SOC effectively, ensuring that all regional data centers are monitored with consistent standards.

ABOUT EXTRAHOP

ExtraHop empowers enterprises to stay ahead of evolving threats with the most comprehensive approach to network detection and response (NDR).

Since 2007, the company has helped organizations across the globe extract real-time insights from their hybrid networks with the most in-depth network telemetry. ExtraHop uniquely combines NDR, network performance monitoring (NPM), intrusion detection (IDS), and packet forensics in a single, integrated console for complete network visibility and unparalleled context that supports data-driven security decisions. With a powerful all-in-one sensor and cloud-scale machine learning, the ExtraHop RevealX™ platform enhances SOC productivity, reduces overhead, and elevates security postures.

Unlock the full power of network detection and response with ExtraHop. To learn more, visit **extrahop.com** or follow us on **LinkedIn**.

EXTRAHOP®

info@extrahop.com
extrahop.com